UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/824,729	04/14/2004	Mark Baugher	50325-0867	6696

29989 7590 12/23/2008
HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
LOUIE, OSCAR A	
ART UNIT	PAPER NUMBER
2436	
MAIL DATE	DELIVERY MODE
12/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/824,729	**Applicant(s)** BAUGHER, MARK	
	Examiner OSCAR A. LOUIE	**Art Unit** 2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 6-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 6-31* is/are rejected.

7)☒ Claim(s) *3-5* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 10/15/2008. Claims 1, 2, & 4-32 are pending and have been considered as follows.

Examiner Note

In light of the applicant's amendments, the examiner hereby withdraws his previous Claim Objection with respect to Claim 18 and withdraws his previous 35 U.S.C. 101 rejection with respect to Claim 17.

Allowable Subject Matter

1. Claims 3-5 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

- The examiner notes that the inclusion of the limitations found under Claims 3-5 into each and every independent claim would place the applicant's application into a much better condition for allowance pending further review;

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 2, 11, 15-20, 24, & 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schuba et al. (US-6944663-B2) in view of French et al. (US-6321339-B1).

Claim 1:

Schuba et al. disclose a method of preventing an attack on a network comprising,

- "receiving a request to access a resource from a user" (i.e. "the system receives a request for service from a client 106 (step 202)") [column 3 lines 52-53];
- "wherein the request includes an accumulated work value" (i.e. "the system generates a random number, y, and a transaction identifier, id.sub.1 (step 204). The system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 53-58];
- "determining whether the accumulated work value exceeds a required work threshold value" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39];

- "if not, requiring the user to perform a quantity of work as a condition for accessing the resource" (i.e. "FIG. 2 is a flow chart illustrating the process of using a client puzzle in accordance with an embodiment of the present invention") [column 3 lines 50-52];
- "providing the user with access to the resource" (i.e. "Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 36-39];
- "determining an amount of accumulated work output value to provide to the user based on a volume of data communicated between the resource and the user" (i.e. "the system generates a random number, y, and a transaction identifier, id.sub.1 (step 204). The system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 53-58];
- "providing the accumulated work output value to the user" (i.e. "The system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 55-58];

but, they do not explicitly disclose,

- "wherein the accumulated work value represents a total amount of work previously performed by the user and accumulated across multiple prior requests by the user," although French et al. do suggest combined authentication scores, as recited below;
- "wherein the accumulated work output value represents a second amount of work performed by the user," although French et al. do suggest combined authentication scores, as recited below;

however, French et al. do disclose,

- "The transaction record 112 (illustrated in FIGS. 13-16) initialized in step 22 is used throughout the authentication process 10 to keep track of user input and authentication results. After the appropriate queries have been processed and all results stored in the transaction record 112, the transaction record 112 is used to determine an authentication score with respect to the request. Step 56 calculates the total authentication score, and optionally, a score for each data source, data field, etc. The results are categorized as a big hit (B), a regular hit (R), a possible hit (P), or no hit (N) depending on results. Those results may then be combined with the results of second level authentication process 40 to determine an overall authenticity certainty score, as illustrated in FIGS. 23-28 and discussed below" [column 14 lines 1-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the accumulated work value represents a total amount of work previously performed by the user and accumulated across multiple prior requests by the user" and "wherein the accumulated work output value represents a second amount of work performed by the user," in the invention as disclosed by Schuba et al. for the purposes of providing categories of access based on values associated with authentication outcomes.

Claim 2:

Schuba et al. and French et al. disclose a method of preventing an attack on a network, as in Claim 1 above, their combination further disclosing,

- "determining whether a mathematical relationship of the current user identity value and the prior user identity value indicates that the user has possession of a resource secret" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39].

but they do not explicitly disclose,

- "wherein the request includes a prior user identity value and a current user identity value," although Schuba et al. do suggest separate identifiers, as recited below;

however, they do disclose,

- "For example, if the parameters associated with the client (id.sub.1, n, y) are stored in a database that is indexed by id.sub.1, a subsequent lookup using id.sub.2 will return (id.sub.1, n, y) only if id.sub.1 =id.sub.2. Alternatively, if the lookup is based on client identifiers, an explicit comparison of id.sub.1 and id.sub.2 needs to be performed" [column 4 lines 29-34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the request includes a prior user identity value and a current user identity value," in the invention as disclosed by Schuba et al. and French et al. since it would be expected that a client/user may attempt to connect more than just once and accommodations need to be made to handle the scenarios where the client is legitimate and non-legitimate as is suggested by Schuba et al.

Claim 11:

Schuba et al. and French et al. disclose a method of preventing an attack on a network, as in Claim 1 above, their combination further disclosing,

- "receiving the accumulated proof of work value" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39].

Claim 15:

Schuba et al. and French et al. disclose a method of preventing an attack on a network, as in Claim 1 above, their combination further disclosing,

- "wherein requiring the user to perform a quantity of work as a condition for accessing the resource comprises requiring the user to hash a message until a specified number of bits are zero" (i.e. "Next, the system stores (id.sub.1, n, y) at server 102 (step 208) and sends (id.sub.1, n, y) to client 106 (step 210). The system then allows client 106 to compute the preimage x, such that h(x)=y (step 212). In one embodiment of the present invention, h is a hash function, such as SHA1 or MD5, so that computing the preimage x given y requires significantly more time than computing the hash function h(x) given x") [column 3 lines 59-64].

Claim 16:

Schuba et al. disclose a method of preventing an attack on a network comprising,

- "receiving a request to access a resource from a user" (i.e. "the system receives a request for service from a client 106 (step 202).") [column 3 lines 52-53];
- "determining whether the accumulated work value exceeds a required work threshold value" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39];
- "providing the user with access to the resource only when the accumulated work value exceeds a required work threshold value" (i.e. "If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 36-39];

but they do not explicitly disclose,

- "wherein the request includes an accumulated work value that represents work that the resource has previously required the user to perform in order to obtain previous access to the resource," although French et al. do suggest combined authentication scores, as recited below;

however, French et al. do disclose,

- "The transaction record 112 (illustrated in FIGS. 13-16) initialized in step 22 is used throughout the authentication process 10 to keep track of user input and authentication results. After the appropriate queries have been processed and all results stored in the transaction record 112, the transaction record 112 is used to determine an authentication score with respect to the request. Step 56 calculates the total authentication score, and optionally, a score for each data source, data field, etc. The results are categorized as a big hit (B), a regular hit (R), a possible hit (P), or no hit (N) depending on results. Those results may then be combined with the results of second level authentication process 40 to determine an overall authenticity certainty score, as illustrated in FIGS. 23-28 and discussed below" [column 14 lines 1-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the request includes an accumulated work value that represents work that the resource has previously required the user to perform in order to obtain previous access to the resource," in the invention as disclosed by Schuba et al. for the purposes of providing categories of access based on values associated with authentication outcomes.

Claims 17-19:

Schuba et al. disclose an apparatus for preventing an attack on a network and a computer-readable volatile or non-volatile medium storing one or more sequences of instructions comprising,

- "a processor" and "one or more processors" (i.e. "a computer system based on a microprocessor, a mainframe computer, a digital signal processor, a portable computing device, a personal organizer, a device controller, and a computational engine within an appliance") [column 3 lines 35-38];

- "a computer-readable volatile or non-volatile medium storing one or more stored sequences of instructions that are accessible to the processor" (i.e. "The data structures and code described in this detailed description are typically stored on a computer readable storage medium, which may be any device or medium that can store code and/or data for use by a computer system. This includes, but is not limited to, magnetic and optical storage devices such as disk drives, magnetic tape, CDs (compact discs) and DVDs (digital versatile discs or digital video discs)") [column 3 lines 10-12];
- "wherein execution of the one or more stored sequences of instructions by the processor causes the processor to perform: receiving a request to access a resource from a user" (i.e. "the system receives a request for service from a client 106 (step 202)") [column 3 lines 52-53];

  "wherein the request includes an accumulated work value" (i.e. "the system generates a random number, y, and a transaction identifier, id.sub.1 (step 204). The system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 53-58];
- "determining whether the accumulated work value exceeds a required work threshold value" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39];

- "if not, requiring the user to perform a quantity of work as a condition for accessing the resource" (i.e. "FIG. 2 is a flow chart illustrating the process of using a client puzzle in accordance with an embodiment of the present invention") [column 3 lines 50-52];
- "providing the user with access to the resource" (i.e. "Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 36-39];
- "determining an amount of accumulated work output value to provide to the user based on a volume of data communicated between the resource and the user" (i.e. "the system generates a random number, y, and a transaction identifier, id.sub.1 (step 204). The
- system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 53-58];
- "providing the accumulated work output value to the user" (i.e. "The system also selects a value for the parameter, n, which specifies the amount of computational work involved in computing the preimage x, such that h(x)=y (step 206)") [column 3 lines 55-58];

but, they do not explicitly disclose,

- "wherein the accumulated work value represents a total amount of work previously performed by the user and accumulated across multiple prior requests by the user," although French et al. do suggest combined authentication scores, as recited below;
- "wherein the accumulated work output value represents a second amount of work performed by the user," although French et al. do suggest combined authentication scores, as recited below;

however, French et al. do disclose,

- "The transaction record 112 (illustrated in FIGS. 13-16) initialized in step 22 is used throughout the authentication process 10 to keep track of user input and authentication results. After the appropriate queries have been processed and all results stored in the transaction record 112, the transaction record 112 is used to determine an authentication score with respect to the request. Step 56 calculates the total authentication score, and optionally, a score for each data source, data field, etc. The results are categorized as a big hit (B), a regular hit (R), a possible hit (P), or no hit (N) depending on results. Those results may then be combined with the results of second level authentication process 40 to determine an overall authenticity certainty score, as illustrated in FIGS. 23-28 and discussed below" [column 14 lines 1-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the accumulated work value represents a total amount of work previously performed by the user and accumulated across multiple prior requests by the user" and "wherein the accumulated work output value represents a second amount of work performed by the user," in the invention as disclosed by Schuba et al. for the purposes of providing categories of access based on values associated with authentication outcomes.

Claims 20, 24, & 28:

Schuba et al. disclose an apparatus for preventing an attack on a network and a computer-readable volatile or non-volatile medium storing one or more sequences of instructions, as in Claims 17-19 above, further comprising,

- "determining whether a mathematical relationship of the current user identity value and the prior user identity value indicates that the user has possession of a resource secret" (i.e. "If id.sub.1 =id.sub.2 at step 218, the system computes h(x) (step 220). Next, the system compares y and h(x) (step 222). If y=h(x), the client successfully solved the client puzzle, and the system performs the requested service for the client (step 224)") [column 4 lines 35-39].

but they do not explicitly disclose,

- "wherein the request includes a prior user identity value and a current user identity value," although Schuba et al. do suggest two separate identifiers, as recited below;

however, they do disclose,

- "For example, if the parameters associated with the client (id.sub.1, n, y) are stored in a database that is indexed by id.sub.1, a subsequent lookup using id.sub.2 will return (id.sub.1, n, y) only if id.sub.1 =id.sub.2. Alternatively, if the lookup is based on client identifiers, an explicit comparison of id.sub.1 and id.sub.2 needs to be performed" [column 4 lines 29-34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the request includes a prior user identity value and a current user identity value," in the invention as disclosed by Schuba et al. since it would be expected that a client/user may attempt to connect more than just once and accommodations need to be made to handle the scenarios where the client is legitimate and non-legitimate as is suggested by Schuba et al.

4. Claims 6-10, 12-14, 21-23, 25-27, & 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schuba et al. (US-6944663-B2) in view of French et al. (US-6321339-B1) and in further view of Juels et al. (US-7197639-B1).

Claim 6:

Schuba et al. and French et al. disclose a method of preventing an attack on a network, as in Claim 3 above, their combination further disclosing, disclose a method of preventing an attack on a network, as in Claim 1 above, but their combination do not explicitly disclose,

- "determining the required work threshold value based on a then-current capacity of the resource," although Juels et al. do suggest computational capacity used to determine computational size, as recited below;

however, Juels et al. do disclose,

- "the rate of connection buffer allocation and the likely computational capacity of one or more attacking clients 110 can be used to select the computational size of a particular tasks when operating in a defensive mode" [column 7 lines 29-33];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining the required work threshold value based on a then-current capacity of the resource," in the invention as disclosed by Schuba et al. and French et al. for the purposes of assessing the likelihood of attack.

Claim 7:

Schuba et al. and French et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but their combination do not explicitly disclose,

- "determining the required work threshold value based on a then-current capacity of the resource," although Juels et al. do suggest computational capacity determining computational size, as recited below;
- "requiring a first user who has an accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource," although Juels et al. do suggest adjusting puzzle size/complexity, as recited below;
- "requiring a second user who has an accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource," although Juels et al. do suggest adjusting puzzle size/complexity, as recited below;
- "wherein the second amount of work is greater than the first amount of work," although Juels et al. do suggest adjusting puzzle size/complexity, as recited below;

however, Juels et al. do disclose,

- "the rate of connection buffer allocation and the likely computational capacity of one or more attacking clients 110 can be used to select the computational size of a particular tasks when operating in a defensive mode" [column 7 lines 29-33];

- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining the required work threshold value based on a then-current capacity of the resource" and "requiring a first user who has an accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource" and "requiring a second user who has an accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource" and "wherein the second amount of work is greater than the first amount of work," in the invention as disclosed by Schuba et al. and French et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claim 8:

Schuba et al. and French et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but their combination do not explicitly disclose,

- "wherein the step of determining an amount of accumulated work output value is performed for a specified user only during a specified time period in which accumulating work is allowed for that specified user," although Juels et al. do suggest puzzle size adjustments, as recited below;

however, Juels et al. do disclose,

- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the step of determining an amount of accumulated work output value is performed for a specified user only during a specified time period in which accumulating work is allowed for that specified user," in the invention as disclosed by Schuba et al. and French et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claim 9:

Schuba et al. and French et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but their combination do not explicitly disclose,

- "wherein the step of determining an amount of accumulated work output value is performed for a specified user only if the current user identity value received from the user is not found in a list of user identity values that were previously received in a specified time period," although Juels et al. do suggest increasing puzzle size in response to an attack, as recited below;

however, Juels et al. do disclose,

- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the step of determining an amount of accumulated work output value is performed for a specified user only if the current user identity value received from the user is not found in a list of user identity values that were previously received in a specified time period," in the invention as disclosed by Schuba et al. and French et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claim 10:

Schuba et al. and French et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but their combination do not explicitly disclose,

- "digitally signing and providing a timestamp to the user with the accumulated work output value," although Juels et al. do suggest time stamping and usage of a secretly computed message authentication code residing as part of the other data, as recited below;

- "wherein the step of determining an amount of accumulated work output value is performed for a specified user," although Juels et al. do suggest client puzzles, as recited below;
- "only upon: receiving the timestamp is received in a subsequent request," although Juels et al. do suggest usage of time stamps, as recited below;
- "only upon: verifying the timestamp value," although Juels et al. do suggest usage of time stamps, as recited below;
- "only upon: determining that the timestamp value is within an allowed range," although Juels et al. do suggest usage of time stamps, as recited below;

however, Juels et al. do disclose,

- "This time stamp, or any other portion of seed data (SD) can be optionally authenticated with the use of a secretly computed message authentication code residing as part of the other data (OD) 530 portion of the seed data (500)" [column 19 lines 22-26];
- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "digitally signing and providing a timestamp to the user with the accumulated work output value" and "wherein the step of determining an amount of accumulated work output value is performed for a specified user" and "only upon: receiving the timestamp is received in a subsequent request" and "only upon: verifying the timestamp value" and "only upon: determining that the timestamp value is within an allowed range," in the invention as disclosed by Schuba et al. and French et al. since "secretly computed message authentication code residing as part of the other data" may typically be "digitally signed and time stamped" information for verification, where a client puzzle protocol is used to control graceful degradation in service.

Claim 12:

Schuba et al. and French et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but their combination do not explicitly disclose,

- "a prior user identity value and a current user identity value in a cookie provided by the user to the resource," although Juels et al. do suggest a client puzzle protocol, as recited below;
- "wherein determining an amount of accumulated work output value to provide to the user based on a volume of data communicated between the resource and the user comprises determining the amount of accumulated work as 2^k * p," although Juels et al. do suggest client puzzles, as recited below;
- "where k is a number of bits of work previously performed by the user and p is a number of messages or packets communicated between the user and the resource," although Juels et al. do suggest client puzzles, as recited below;

however, Juels et al. do disclose,

- "the "client puzzle" protocol" [column 8 line 65];

- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a prior user identity value and a current user identity value in a cookie provided by the user to the resource" and "wherein determining an amount of accumulated work output value to provide to the user based on a volume of data communicated between the resource and the user comprises determining the amount of accumulated work as 2^k * p" and "where k is a number of bits of work previously performed by the user and p is a number of messages or packets communicated between the user and the resource," in the invention as disclosed by Schuba et al. and French et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claim 13:

Schuba et al. and French et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but their combination do not explicitly disclose,

- "providing the accumulated work output value in a cookie sent from the resource to the user," although Juels et al. do suggest client puzzles, as recited below;

however, Juels et al. do disclose,

- "the "client puzzle" protocol" [column 8 line 65];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "providing the accumulated work output value in a cookie sent from the resource to the user," in the invention as disclosed by Schuba et al. and French et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claim 14:

Schuba et al. and French et al. disclose a method of preventing an attack on a network, as in Claim 1 above, but their combination do not explicitly disclose,

- "selectively increasing the required work threshold value for a particular user in response to congestion conditions of the resource," although Juels et al. do suggest adjusting client puzzle size in response to an attack, as recited below;

however, Juels et al. do disclose,

- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "selectively increasing the required work threshold value for a particular user in response to congestion conditions of the resource," in the invention as disclosed by Schuba et al. and French et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Claims 21-23, 25-27, & 29-31:

Schuba et al. and French et al. disclose an apparatus and a computer-readable storage medium storing one or more sequences of instructions, as in Claims 17-19 above, but their combination do not explicitly disclose,

- "determining the required work threshold value based on a then-current capacity of the resource," although Juels et al. do suggest computational capacity, as recited below;
- "requiring a first user who has an accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource," although Juels et al. do suggest client puzzles, as recited below;
- "requiring a second user who has an accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource," although Juels et al. do suggest client puzzles, as recited below;
- "wherein the second amount of work is greater than the first amount of work," although Juels et al. do suggest client puzzles, as recited below;
- "determining an amount of accumulated work output value is operable for a specified user only if the current user identity value received from the user is not found in a list of user identity values that were previously received in a specified time period," although Juels et al. do suggest client puzzles, as recited below;

- "digitally signing and providing a timestamp to the user with the accumulated work output value," although Juels et al. do suggest time stamping and usage of a secretly computed message authentication code residing as part of the other data, as recited below;
- "determining an amount of accumulated work output value is operable for a specified user only upon: receiving the timestamp is received in a subsequent request," although Juels et al. do suggest usage of time stamps, as recited below;
- "verifying the timestamp value," although Juels et al. do suggest usage of time stamps, as recited below;
- "determining that the timestamp value is within an allowed range," although Juels et al. do suggest usage of time stamps, as recited below;

however, Juels et al. do disclose,

- "the rate of connection buffer allocation and the likely computational capacity of one or more attacking clients 110 can be used to select the computational size of a particular tasks when operating in a defensive mode" [column 7 lines 29-33];
- "The client puzzle protocol also allows for graceful degradation in service when an attack is mounted. The size of the puzzles can be increased as the progress of an attack advances closer to disabling the server. This enables the protocol to flex according to the scale of the attack" [column 9 lines 10-14];
- "inside each correct sub-puzzle solution, and comparing the time stamp (DT) with the current time to check that the (sub)puzzle has not yet expired" [column 19 lines 20-22];

- "This time stamp, or any other portion of seed data (SD) can be optionally authenticated with the use of a secretly computed message authentication code residing as part of the other data (OD) 530 portion of the seed data (500)" [column 19 lines 22-26];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining the required work threshold value based on a then-current capacity of the resource" and "requiring a first user who has an accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource" and "requiring a second user who has an accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource" and "wherein the second amount of work is greater than the first amount of work" and "determining an amount of accumulated work output value is operable for a specified user only if the current user identity value received from the user is not found in a list of user identity values that were previously received in a specified time period" and "digitally signing and providing a timestamp to the user with the accumulated work output value" and "determining an amount of accumulated work output value is operable for a specified user only upon: receiving the timestamp is received in a subsequent request" and "verifying the timestamp value" and "determining that the timestamp value is within an allowed range," in the invention as disclosed by Schuba et al. and French et al. since the client puzzle protocol is used for controlling the rate of connection buffer allocation and the likely computational capacity in order to provide graceful degradation in service when an attack is mounted (i.e. denial of service attack).

Response to Arguments

5. Applicant's arguments filed 10/15/2008 have been fully considered but they are not persuasive with respect to Claims 1 & 16.

- The applicant's argument, "French contains no suggestion that using the method of authentication described therein would be useful as part of a proof-of-work approach to protect against denial of service attacks," has been carefully considered but is non-persuasive since whether the prior art states that it would be useful for the same purpose or not useful for the same purpose as the applicant's claimed invention is not a persuasive argument, since it is still a proof of work approach regardless whether it is useful/not useful against denial of service attacks; See below:

> *Disclosed examples and preferred embodiments do not constitute a teaching away from a broader disclosure or nonpreferred embodiments. In re Susi, 440 F.2d 442, 169 USPQ 423 (CCPA 1971). "A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use." In re Gurley, 27 F.3d 551, 554, 31 USPQ2d 1130, 1132 (Fed. Cir. 1994) (The invention was directed to an epoxy impregnated fiber-reinforced printed circuit material. The applied prior art reference taught a printed circuit material similar to that of the claims but impregnated with polyester-imide resin instead of epoxy. The reference, however, disclosed that epoxy was known for this use, but that epoxy impregnated circuit boards have "relatively acceptable dimensional stability" and "some degree of flexibility," but are inferior to circuit boards impregnated with polyester-imide resins. The court upheld the rejection concluding that applicant's argument that the reference teaches away from using epoxy was insufficient to overcome the rejection since "Gurley asserted no discovery beyond what was known in the art." 27 F.3d at 554, 31 USPQ2d at 1132.). Furthermore, "[t]he prior art's mere disclosure of more than one alternative does not constitute a teaching away from any of these alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed...." In re Fulton, 391 F.3d 1195, 1201, 73 USPQ2d 1141, 1146 (Fed. Cir. 2004).*

- The applicant's argument, "Schuba fails to teach or suggest "receiving a request to access a resource from a user, wherein the request includes an accumulated work value"," has been carefully considered but is non-persuasive since Schuba does suggest an amount of computational work involved to be computed where it would have been reasonable to expect any amount of computational work to be computed;
- The applicant's argument, "French fails to teach or suggest "multiple prior requests by the user"," has been carefully considered but is non-persuasive since it is reasonable to expect a user to have one or more requests over any given period of time;
- The applicant's argument, "French fails to teach or suggest "wherein the accumulated work value represents a total amount of work previously performed by the user and accumulated across multiple prior requests by the user"," has been carefully considered but is non-persuasive since French does disclose if not at the very least suggest utilizing a form of authentication score which is tracked;
- The applicant's arguments, "Schuba does not teach an "accumulated work value" or a "required work threshold value" in any way. Also, determining if "the client successfully solved the client puzzle" as recited by Schuba does not equate to "determining whether the accumulated work value exceeds a required work threshold value" as recited by Claim 1. Because Schuba fails to teach "determining whether the accumulated work value exceeds a required work threshold value"" and "determining if "the client successfully solved the client puzzle" as recited by Schuba does not equate to "determining whether the accumulated work value exceeds a required work threshold value"" and "Schuba fails to teach or suggest "determining whether the accumulated

work value exceeds a required work threshold value" as recited by Claim 16. Thus, it is impossible that Schuba discloses "providing the user with access to the resource only when the accumulated work value exceeds a required work threshold value"," have been carefully considered but is non-persuasive since Schuba does disclose if not suggest a proof of work/puzzle type of solution where a client successfully solving a puzzle implies that whatever the threshold is set as, it has been met or exceeded since the puzzle was completed correctly;

- The applicant's argument, "Schuba fails to teach or describe "determining an amount of accumulated work output value to provide to the user based on a volume of data communicated between the resource and the user"," has been carefully considered but is non-persuasive since Scuba does disclose if not suggest an amount of computation work to be performed based on a formula where it is reasonable to expect a variety of inputs that are used as part of the calculation;
- The applicant's argument, "French fails to teach or describe "wherein the accumulated work output value represents a second amount of work performed by the user"," has been carefully considered but is non-persuasive since is it reasonable to expect that if a user performs computations for one amount of work, they could perform any additional amount of computation of work;
- The applicant's argument, "Schuba fails to teach an "accumulated work output value" recited by Claim 1. Therefore, it is impossible that Schuba teaches or suggests "providing the accumulated work output value to the user"," has been carefully considered but is

non-persuasive since it is reasonable to expect an amount of calculated work that is a culmination of different accumulated variables for a user to perform a proof of work on;

- The applicant's arguments, "any work being done to obtain access to a resource in French does not include "work that the resource has previously required the user to perform in order to obtain previous access to the resource"" and "Schuba fails to teach or suggest a request from a client that "includes an accumulated work value that represents work that the resource has previously required the user to perform in order to obtain previous access to the resource,"" have been carefully considered but is non-persuasive since French suggests keeping track of authentication scores of a user to determine if the user has previously been successfully authenticated;

6. Applicant's arguments with respect to claims 17-31 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicant's amendments.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
12/19/2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436